



**Commonwealth of Massachusetts
Electronic Payment Processing Services Contract
(PRF44designatedOSC)
and PCI Compliance (CTRPCI2007)
General Information
March 2011**

Part of the Commonwealth's E-Government Initiative includes a program for accepting electronic payments from customers. The Statewide Contract for Electronic Payment Processing Services (PRF44designatedOSC), gives eligible Commonwealth entities the option to offer their customers a variety of payment methods. Customers may pay for goods, services and other obligations via ACH and credit cards (VISA, MasterCard, Discover and/or American Express), and with PIN debit cards. The "ePay" transactions can be processed over the web, over the phone via Interactive Voice Response (IVR), or in person using point of sale hardware. The Office of the Comptroller, with designation from the Operational Services Division, administers the contract.

Vendors

The vendors currently selected under this contract are:

1. HP -- provides the web and IVR applications, and access to the ACH banking network;
2. Bank of America (BoA) -- provides credit card processing for VISA, MasterCard, and Discover; and
3. American Express (Amex) – processes American Express branded credit card transactions.

Contract Duration

This contract runs through June 30, 2013 with annual options to renew through June 30, 2015 (two option years).

Applicable Procurement Laws

MGL c. 7, § 22; c. 30, § 51, § 52; 801 CMR 21.00 and 808 CMR 1.00

Eligible Entities

All eligible entities' transactions processed under this Statewide Contract will be included in the Commonwealth's purchasing totals, which with increased use may result in volume discounts for the Commonwealth.

- Required Users: Executive Offices, Departments, Agencies, Offices, Divisions, Boards, Commissions, or Institutions within the Executive Branch.
- Optional Users: The Legislative Branch, the Judicial Branch, the Constitutional Offices, Elected Offices, Public Institutions of Higher Education, and the Military Division are not required, but may choose to use this Statewide Contract. Cities,

towns, municipalities and State Authorities may also choose use this Statewide Contract.

Services Provided

A Department may select one or more services from the contract menu depending on their business requirements. This ranges from web-based payment to credit card processing to automatic CR generation in MMARS. Below is a brief description of these various options:

1. **Web-Based Processing** – provided by HP and one or more acquirers (Bank of America, American Express). The HP/acquirer solution consists of the following functional areas:

- HP hosts and supports a range of options for Departments to establish and offer web and/or Interactive Voice Response (IVR) applications.
- Bank of America (Visa, Mastercard, and Discover) and Amex provide the credit card processing component.
- HP partners with Bank of America to process ACH payments.

For online credit card payments the customer must enter the credit card number, expiration date, and three-digit code from the signature field on the back of the card. For online ACH payments, the customer must enter their bank account, routing number, and other required information. Currently, debit cards are not accepted over the Internet for most industries.

2. **Non-Web-based Payment Processing** -- If a department does not wish to offer an on-line payment solution they can still offer payment via credit card, debit card, and ACH. At the point of sale, departments may implement credit card swipe terminals or pin debit payment acceptance programs. Credit card and ACH payments can also be accepted via Interactive Voice Response (IVR), which can be customized according to department specifications.

The range of services HP provides, in partnership with BoA for Visa, Mastercard, Discover, and ACH, and with American Express includes:

- Acquiring transactions through the Internet and/or IVR (interactive voice response), if required (see above).
- Forwarding authorization requests to the card issuing banks.
- Returning confirmation of authorization approvals to the customers.
- Validating bank routing and transit numbers.
- Forwarding MasterCard and VISA transaction data for clearing and settlement with the bankcard associations.
- Forwarding Discover and American Express transaction data to the respective card companies for clearing and settlement.

- Forwarding ACH transactions in standard NACHA formats to ACH financial institutions.
- Providing to the Commonwealth all remittance data files and financial control reports corresponding to the Internet and/or IVR transactions.

Value to the Commonwealth

The value to the Commonwealth in contracting with HP to perform these services includes the following benefits:

- Wide range of service levels and mix of payment methods offered.
- Web sites customized to Departments' needs, if needed.
- 24 x 7 technical support of the payment system -- Departments do not need staff to maintain the system.
- Capacity to handle increasing volumes, as well as peaks in payments.
- Files sent to update the Departments' accounts receivable or billing systems as well as updates to MMARS.
- Complete end-to-end reporting.
- Fraud prevention.
- Secure storage data.
- Pay-by-phone scripts customized to Departments' needs.
- Ease of reconciliation.

Fees and Departmental Responsibilities

Each individual Commonwealth Department requesting and accepting electronic payment processing (e-payment) services shall be solely legally responsible for payment of that Department's obligations under the Contract, subject to sufficient appropriations and allotments, and the Contractor(s) may not seek payment of such obligations from the Office of the State Comptroller or any other Commonwealth Department, nor shall any Commonwealth Department have any legal obligation to make payments for e-payment services other than the Department requesting and accepting such services.

When a Department agrees to accept e-payment services, the Department certifies that prior to the beginning of each fiscal year, and during the fiscal year, the Department shall be responsible for taking the necessary steps to ensure that there are sufficient funds for payment of these e-payment fees and chargebacks. Departments should work with the electronic payment processing Contractor(s) to determine an estimated amount of fees and other costs for each fiscal year based upon historical or anticipated e-payment usage. Departments will be required to encumber or set aside, at a minimum, this estimated amount of funds for e-payment fees and costs. Departments will be required to suspend acceptance of e-payments whenever the Department anticipates not having sufficient funds for e-payment fees and costs. Seeking funding after the fact through the deficiency process or prior year deficiency process shall not be considered an appropriate funding mechanism.

Departments can choose which payment options they want to use; they are not required by the contract to offer all forms of payment or credit card types. In addition, the same Department may have different programs requiring different payment solutions, card types, etc., all of which can be accommodated.

Calculating the fees to be charged when using electronic payment processing services can be complicated. Department interested in using the Contractors should go to the contract's website which is available at www.comm-pass.com and search for PRF44designatedOSC.

PCI Compliance

The PCI DSS is a mandatory compliance program of the major credit card associations to create common industry security requirements for cardholder data. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This section provides information about our approach in meeting this challenge.

When accepting credit cards, each Commonwealth entity operates as a “merchant”. All Commonwealth entities that process transmit, or store electronic payments data must adhere to the standard. If your department accepts electronic payments via any means (e.g., mail, cashier window, swipe terminal, kiosk, telephone, or the web), then adherence to these standards is mandatory under current Comptroller policy.

The primary focus of the PCI standards is to help merchants (in our case, Commonwealth Departments) improve the safekeeping of electronic payments information by tightening overall security. This overall review reduces the chances of experiencing security breaches, fraud, and potential catastrophic financial losses, penalties, and loss of trust in Commonwealth public facing applications. Merchants found to be non-compliant with the respective security requirements may be subject to substantial fines and penalties in the event of a data breach. More information about PCI Compliance can be found at <https://www.pcisecuritystandards.org/>.

During 2007, CTR formed a procurement management team with ITD and other departments. Two qualified vendors were engaged to provide consulting, validation, and network scanning services to Commonwealth entities -- Lighthouse Computer Services, Inc. (LCS) and Digital Resources Group, LLC (DRG). Both vendors are certified Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs). Departments must engage one of these vendors to validate their annual PCI compliance activity on an ongoing basis.

The PCI Compliance contract (CTRPCI2007) is a single department procurement/multi-department user contract, not a master service agreement. For audit purposes, the contract will be administered through CTR.

It is of the utmost importance to have citizens feel secure about transacting electronic business with the Commonwealth. The PCI compliance initiative will enable us to ensure that we are doing all we can to protect our citizen's sensitive credit card information.

For additional information or to participate:

For more information or to participate in either contract, contact Patricia Davis, Office of the State Comptroller, One Ashburton Place, 9th floor, Boston, MA 02108, 617-973-2332, Patricia.Davis@state.ma.us. We will meet with you to discuss your business requirements in more detail and suggest the approach that best fits your department's needs.